SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# A Framework for Implementing and Measuring SwA Assurance Process

Michele Moss, Booz Allen Hamilton

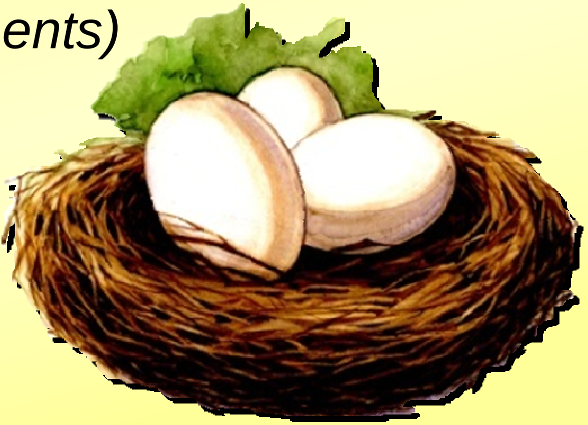
Co-Chair Processes and Practices Working Group

September 29, 2010

# The Solution Requires A Balance Of Benchmarks

- *The chicken…. (a.k.a. Process Focused Assessment )*
  - *Management Systems (ISO 9001, ISO 27001, ISO 2000)*
  - *Capability Maturity Models (CMMI, RMM, SSE-CMM )*
  - *Lifecycle Processes (ISO/IEEE 15288, ISO/IEEE 12207)*
  - *COBIT, ITIL, MS SDL, OSAMM, BSIMM*

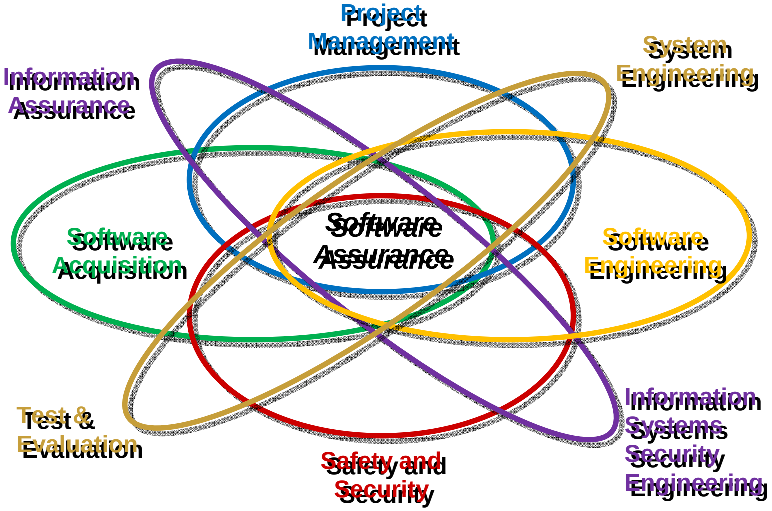
- *The egg … (a.k.a Product Focused Assessments)*
  - *SCAP*
  - *OWASP Top 10*
  - *SANS TOP 25*
  - *OMG and W3C*
  - *Secure Code Check Lists*
  - *Static Code Analysis*
  - *Pen Test Results*



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# *SwA Requires Multi-disciplinary Collaboration*

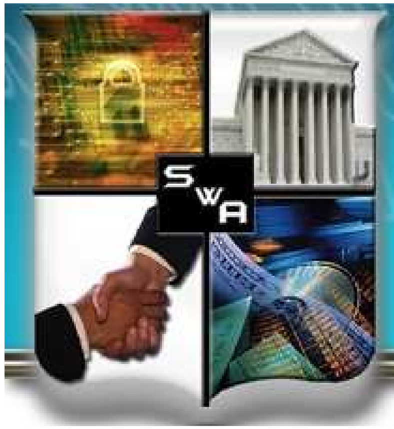


Source: https://buildsecurityin.us-cert.gov/swa/procresrc.html

## Communication Challenges

- Vocabulary
- Reserved Words
- Priorities
- Perspective
- Experience
- Objectives
- Drivers
- Risks

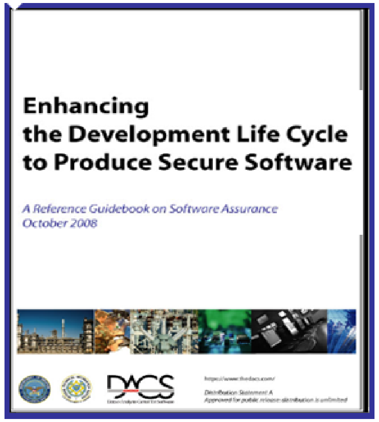
**Without a common language we cannot communicate across disciplines**



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# *Current SwA Communication Tools Focus On Development Focused Audiences*



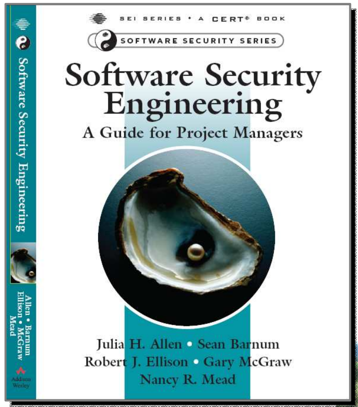
**Enhancing the Development Life Cycle to Produce Secure Software**

*A Reference Guidebook on Software Assurance*
*October 2008*

DACS

https://www.thedacs.com/

Distribution Statement A
Approved for public release: distribution is unlimited



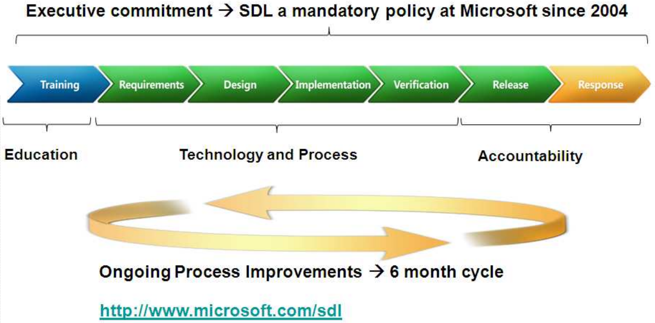
SEI SERIES • A CERT® BOOK

SOFTWARE SECURITY SERIES

Software Security Engineering

A Guide for Project Managers

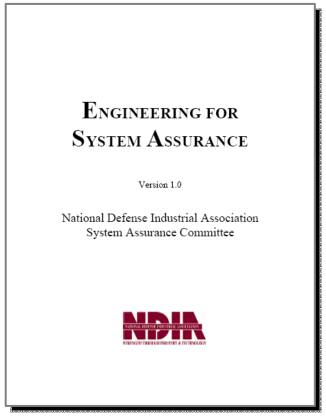
Julia H. Allen • Sean Barnum
Robert J. Ellison • Gary McGraw
Nancy R. Mead



Executive commitment → SDL a mandatory policy at Microsoft since 2004

Ongoing Process Improvements → 6 month cycle

http://www.microsoft.com/sdl



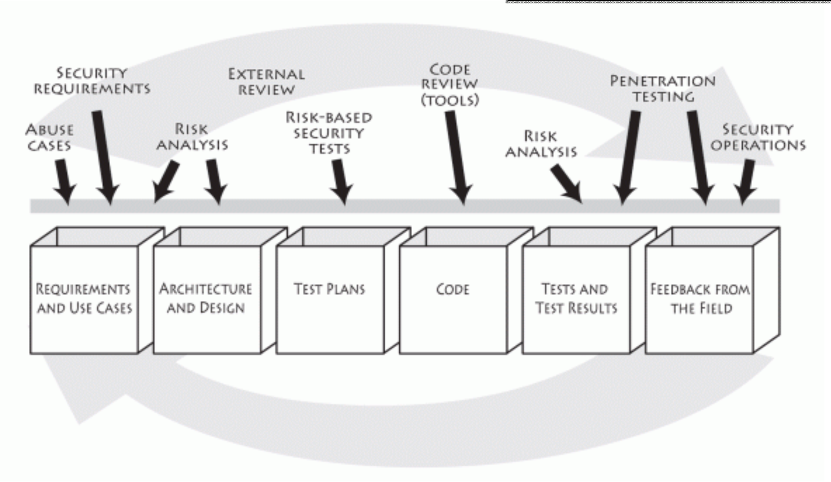
ENGINEERING FOR SYSTEM ASSURANCE

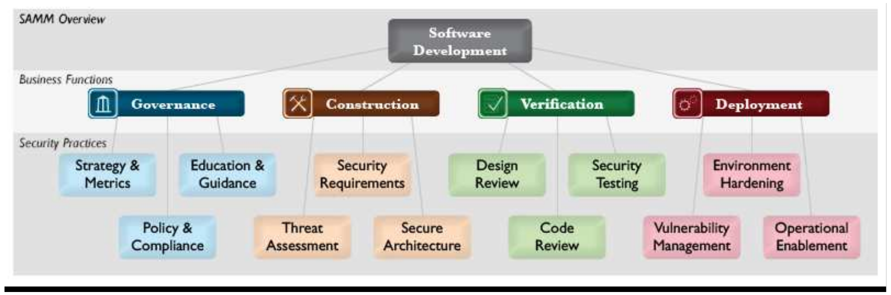
Version 1.0

National Defense Industrial Association
System Assurance Committee

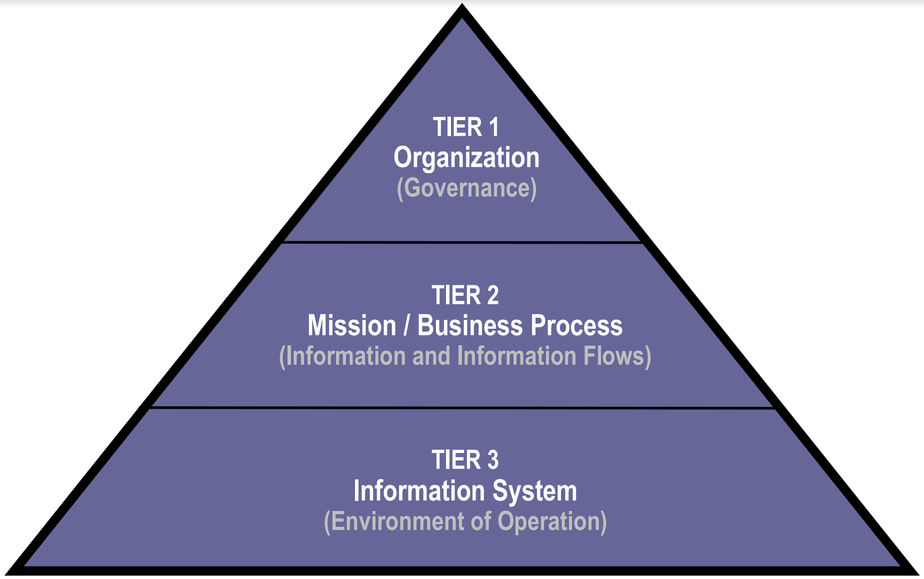
NDIA

Assurance for CMMI ®





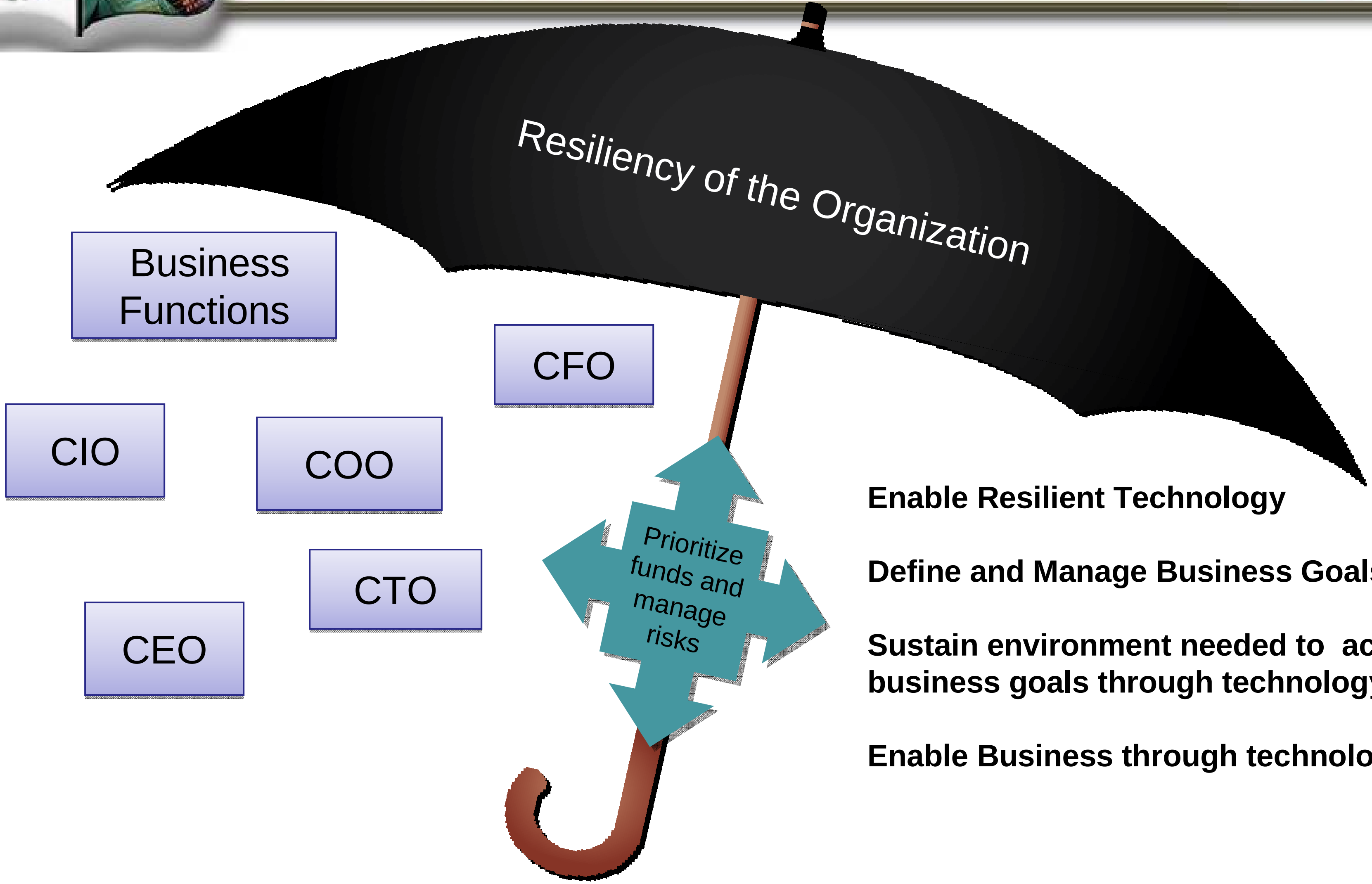
# *SwA Must Translate to Organizational and Mission/ Business Focused Stakeholders*


TIER 1
Organization
(Governance)
TIER 2
Mission / Business Process
(Information and Information Flows)
TIER 3
Information System
(Environment of Operation)

*Source: NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach*

**In a way that is applicable in diverse contexts (Defense, National Security, Finance, Heath care, Aviations, Telecommunications) and is not a source of liability or misunderstanding in acquisition decisions**

# *To connect SwA to the Organization it must translate to the Mission /Business*



Resiliency of the Organization

Business Functions

CFO

CIO

COO

CTO

CEO

Prioritize funds and manage risks

**Enable Resilient Technology**

**Define and Manage Business Goals**

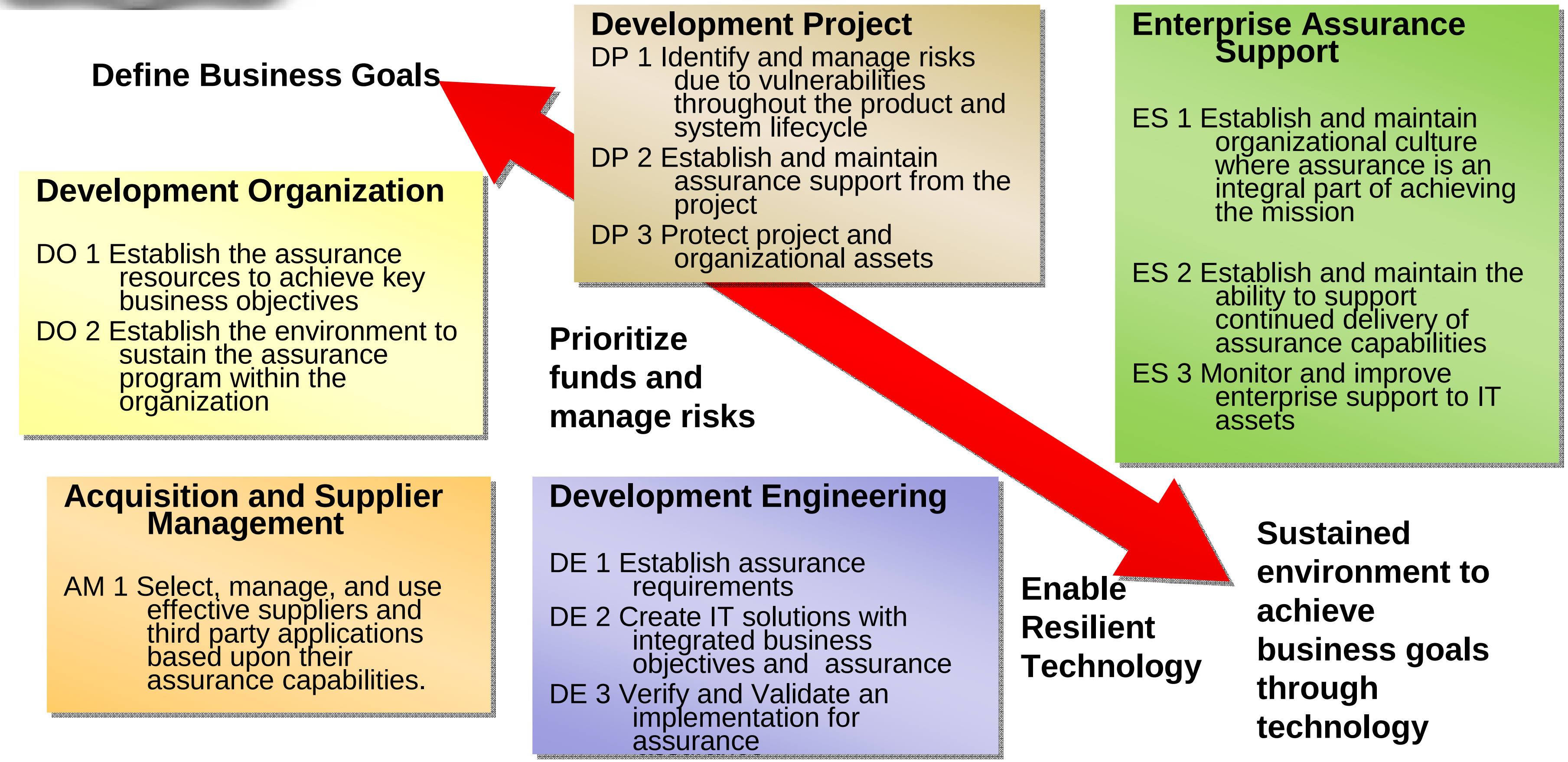
**Sustain environment needed to achieve business goals through technology**

**Enable Business through technology**

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# *The Assurance PRM is a Holistic Framework*



**Define Business Goals**

### Development Project

DP 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle

DP 2 Establish and maintain assurance support from the project

DP 3 Protect project and organizational assets

### Enterprise Assurance Support

ES 1 Establish and maintain organizational culture where assurance is an integral part of achieving the mission

ES 2 Establish and maintain the ability to support continued delivery of assurance capabilities

ES 3 Monitor and improve enterprise support to IT assets

### Development Organization

DO 1 Establish the assurance resources to achieve key business objectives

DO 2 Establish the environment to sustain the assurance program within the organization

**Prioritize funds and manage risks**

### Acquisition and Supplier Management

AM 1 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

### Development Engineering

DE 1 Establish assurance requirements

DE 2 Create IT solutions with integrated business objectives and assurance

DE 3 Verify and Validate an implementation for assurance

**Enable Resilient Technology**

**Sustained environment to achieve business goals through technology**

***Created to facilitate Communication Across An Organization's Multi-Disciplinary Stakeholders***

https://buildsecurityin.us-cert.gov/swa/proself_assm.html

# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

*https://buildsecurityin.us-cert.gov/swa/proself_assm.html*

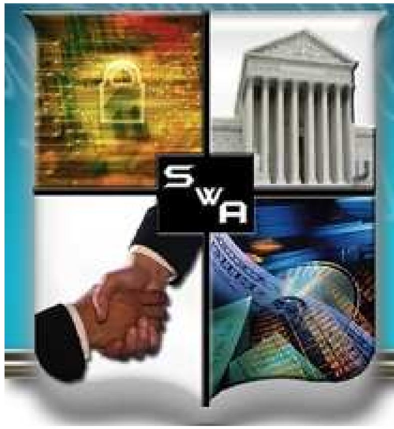
The DHS SwA Processes and Practices Working Group has synthesized the contributions of leading government and industry experts into a set of high-level goals and supporting practices (an evolution of the SwA community's Assurance Process Reference Model)

The goals and practices are mapped to specific industry resources providing additional detail and real world implementation and supporting practices

- Assurance Focus for CMMI
- Building Security In Maturity Model
- Open Software Assurance Maturity Model
- CERT® Resilience Management Model
- CMMI for Acquisition
- CMMI for Development
- CMMI for Services
- SwA Community's Assurance Process Reference Model –Initial Mappings
- SwA Community's Assurance Process Reference Model - Self Assessment
- SwA Community's Assurance Process Reference Model – Mapping to Assurance Models

Other valuable resources that are in the process of being mapped include

- NIST IR 7622: DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems
- NDIA System Assurance Guidebook
- Microsoft Security Development Lifecycle
- SAFECode

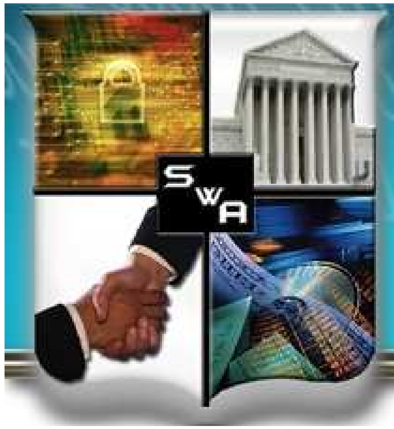


## Process Reference Model for Assurance – Goals and Practices September 2010

In the following table, all references to “assurance” are intended to include system and software assurance, information assurance, and cyber security in support of the business/mission functions supported by systems and software.

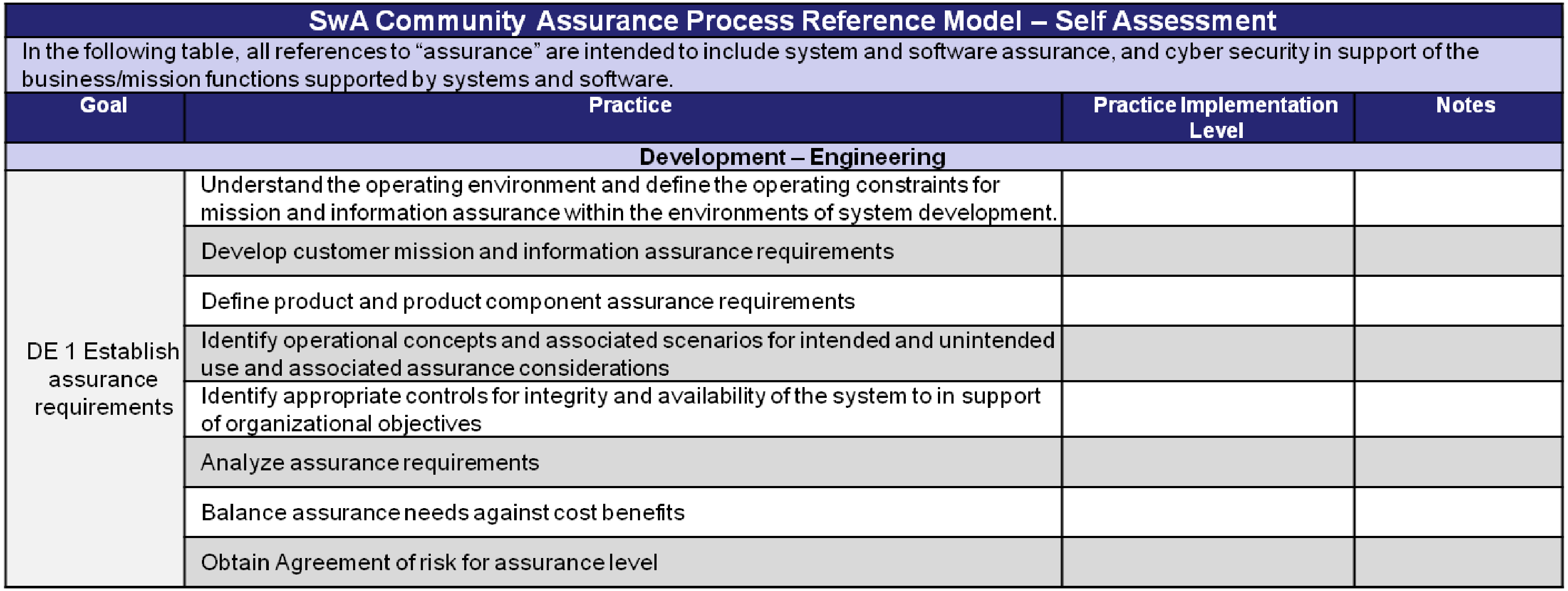
| Goal | Practice List |
|---|---|
| **Development – Engineering** | |
| DE 1 Establish assurance requirements | Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development. |
| | Develop customer mission and information assurance requirements |
| | Define product and product component assurance requirements |
| | Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations |
| | Identify appropriate controls for integrity and availability of the system to in support of organizational objectives |
| | Analyze assurance requirements |
| | Balance assurance needs against cost benefits |
| | Obtain Agreement of risk for assurance level |

https://buildsecurityin.us-cert.gov/swa/proself_assm.html



# *It can be used by acquirers, suppliers and integrators as a to tool to discuss areas of strength and weakness*

- What assurance goals are being met?
- What practices are being implemented?
- Who are the suppliers and how are they managing risk?



**SwA Community Assurance Process Reference Model – Self Assessment**

In the following table, all references to “assurance” are intended to include system and software assurance, and cyber security in support of the business/mission functions supported by systems and software.

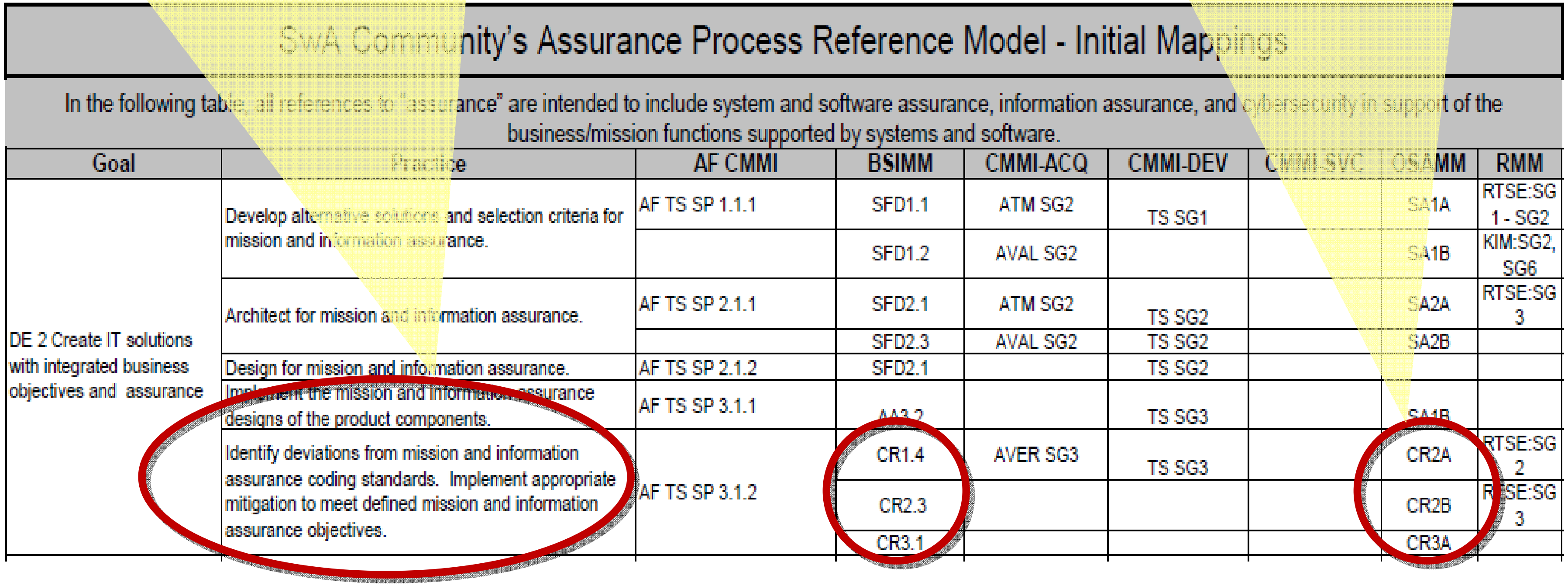
| Goal | Practice | Practice Implementation Level | Notes |
|---|---|---|---|
| | **Development – Engineering** | | |
| DE 1 Establish assurance requirements | Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development. | | |
| | Develop customer mission and information assurance requirements | | |
| | Define product and product component assurance requirements | | |
| | Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations | | |
| | Identify appropriate controls for integrity and availability of the system to in support of organizational objectives | | |
| | Analyze assurance requirements | | |
| | Balance assurance needs against cost benefits | | |
| | Obtain Agreement of risk for assurance level | | |

https://buildsecurityin.us-cert.gov/swa/proself_assm.html

# *It can be used as a navigation tool to guide SwA implementation efforts*

You have been asked to ensure that the OWASP Top Ten (an assurance coding Standard) are not in the Code

You can look at the OSAMM for guidance on how to do it



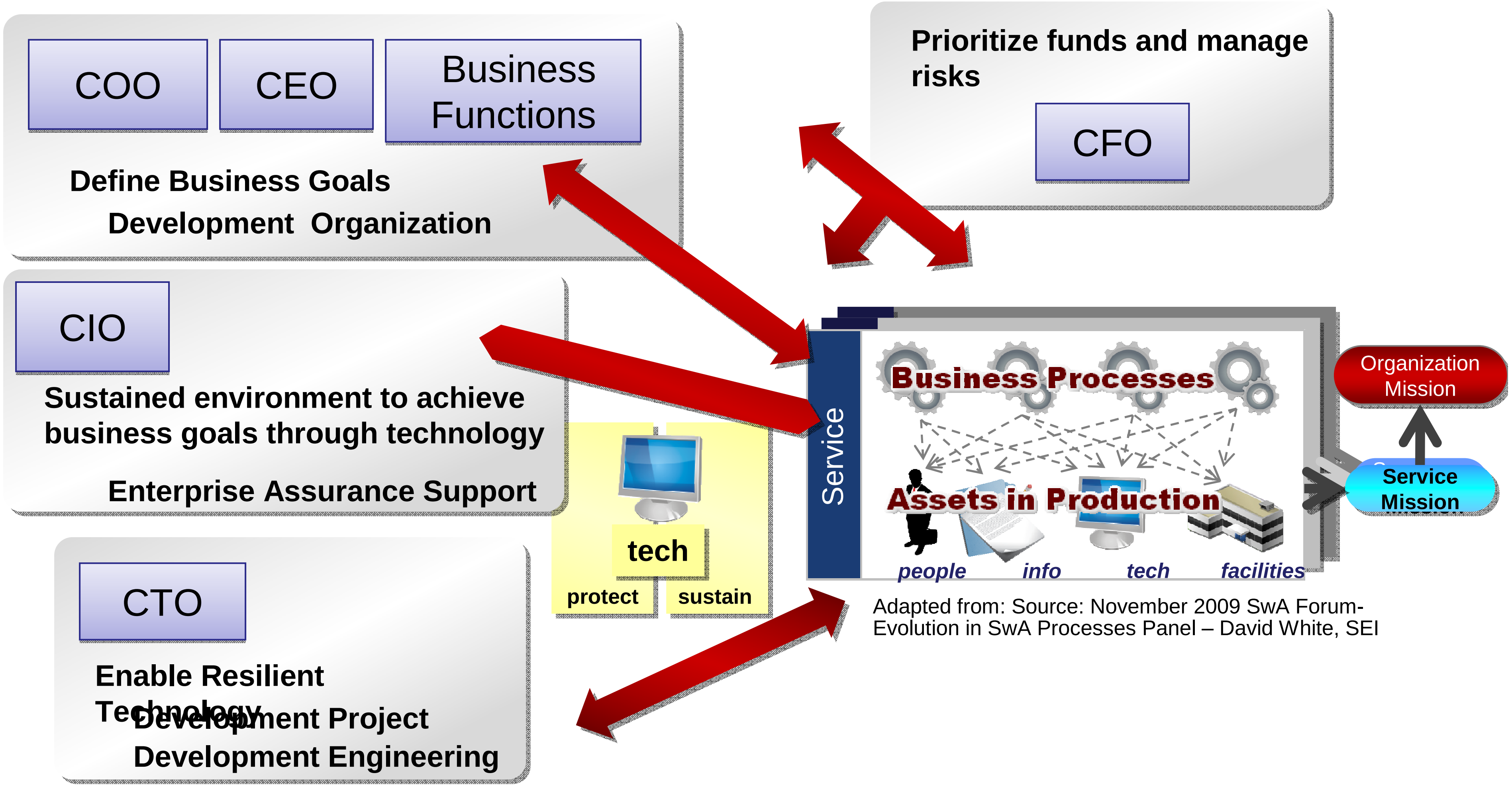
## SwA Community's Assurance Process Reference Model - Initial Mappings

In the following table, all references to "assurance" are intended to include system and software assurance, information assurance, and cybersecurity in support of the business/mission functions supported by systems and software.

| Goal | Practice | AF CMMI | BSIMM | CMMI-ACQ | CMMI-DEV | CMMI-SVC | OSAMM | RMM |
|---|---|---|---|---|---|---|---|---|
| DE 2 Create IT solutions with integrated business objectives and assurance | Develop alternative solutions and selection criteria for mission and information assurance. | AF TS SP 1.1.1 | SFD1.1 | ATM SG2 | TS SG1 | | SA1A | RTSE:SG 1 - SG2 |
| | | | SFD1.2 | AVAL SG2 | | | SA1B | KIM:SG2, SG6 |
| | Architect for mission and information assurance. | AF TS SP 2.1.1 | SFD2.1 | ATM SG2 | TS SG2 | | SA2A | RTSE:SG 3 |
| | | | SFD2.3 | AVAL SG2 | TS SG2 | | SA2B | |
| | Design for mission and information assurance. | AF TS SP 2.1.2 | SFD2.1 | | TS SG2 | | | |
| | Implement the mission and information assurance designs of the product components. | AF TS SP 3.1.1 | AA3.2 | | TS SG3 | | SA1B | |
| | Identify deviations from mission and information assurance coding standards. Implement appropriate mitigation to meet defined mission and information assurance objectives. | AF TS SP 3.1.2 | CR1.4 | AVER SG3 | TS SG3 | | CR2A | RTSE:SG 2 |
| | | | CR2.3 | | | | CR2B | RTSE:SG 3 |
| | | | CR3.1 | | | | CR3A | |

https://buildsecurityin.us-cert.gov/swa/proself_assm.html

*It can be used to begin the translation of SwA Activities across organizational leadership*



COO | CEO | Business Functions

**Define Business Goals**

**Development Organization**

**Prioritize funds and manage risks**

CFO

CIO

**Sustained environment to achieve business goals through technology**

**Enterprise Assurance Support**

CTO

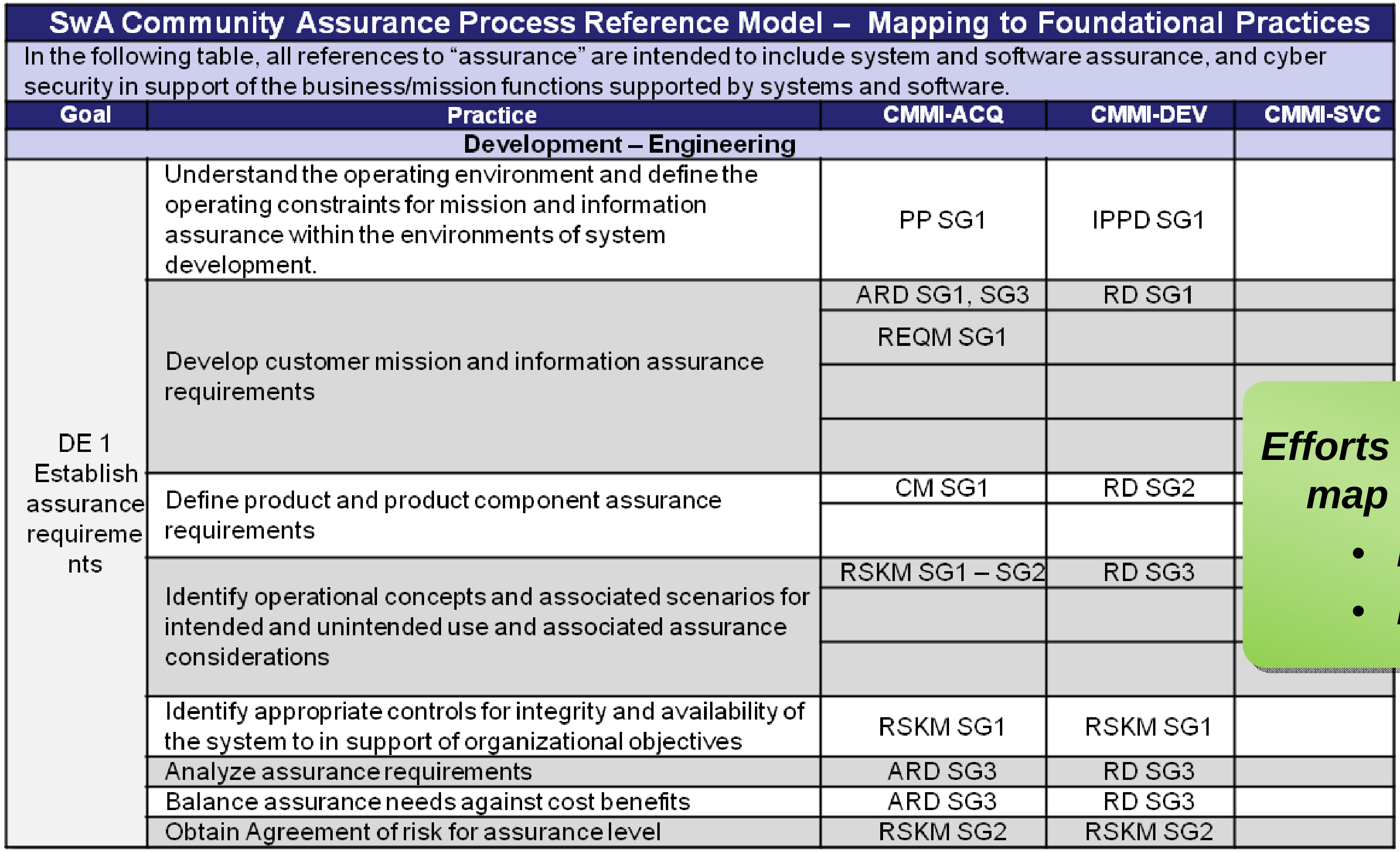
**Enable Resilient Technology**

**Development Project**

**Development Engineering**

Adapted from: Source: November 2009 SwA Forum- Evolution in SwA Processes Panel – David White, SEI

# It can be used to begin the translation of SwA to other across disciplines



**SwA Community Assurance Process Reference Model – Mapping to Foundational Practices**

In the following table, all references to "assurance" are intended to include system and software assurance, and cyber security in support of the business/mission functions supported by systems and software.

| Goal | Practice | CMMI-ACQ | CMMI-DEV | CMMI-SVC |
|---|---|---|---|---|
| | **Development – Engineering** | | | |
| DE 1 Establish assurance requirements | Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development. | PP SG1 | IPPD SG1 | |
| | Develop customer mission and information assurance requirements | ARD SG1, SG3 | RD SG1 | |
| | | REQM SG1 | | |
| | | | | |
| | | | | |
| | Define product and product component assurance requirements | CM SG1 | RD SG2 | |
| | | | | |
| | Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations | RSKM SG1 – SG2 | RD SG3 | |
| | | | | |
| | | | | |
| | Identify appropriate controls for integrity and availability of the system to in support of organizational objectives | RSKM SG1 | RSKM SG1 | |
| | Analyze assurance requirements | ARD SG3 | RD SG3 | |
| | Balance assurance needs against cost benefits | ARD SG3 | RD SG3 | |
| | Obtain Agreement of risk for assurance level | RSKM SG2 | RSKM SG2 | |

***Efforts are underway to map to***

- ***ISO/IEEE 15288***
- ***ISO/IEEE 12207***

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# *Join us at SwA Working Group Events*

**https://buildsecurityin.us-cert.gov/bsi/events.html**

Paul R. Croll
CSC
5166 Potomac Drive
King George, VA  22485-5824

Phone: +1 540.644.6224
Fax: +1 540.663.0276
e-mail: pcroll@csc.com

Michele Moss
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA  22102

Phone: +1 703.377.1254
Fax: +1 703.902.3595
e-mail: moss_michele@bah.com